インターネットPBNM実現に向けたポリシーに基づくドメイン管理方式の実装方法の検討

小田切　和也（椙山女学園大学文化情報学部）

要旨

既存のPolicy-based Network Management (PBNM)方式に対して，著者はDestination Addressing Control System (DACS)方式と呼ぶ方式を提案し，その実現に必要なソフトウェアの研究を進めてきた。このDACS方式は，クライアント上だけにソフトウェア形態の通信制御点（PEP）を配置し，当該クライアントから発信される通信を，そのPEPで制御することでLAN全体を効率的に管理する方式である。本論文では，まず，最初に，既存のDACS方式の内容説明を行う。その後，既存のDACS方式を応用し，各組織が保有するネットワークを複数集めた「複数ネットワーク群」を管理する方式の管理範囲を更に拡張した「ドメイン管理方式」のコンセプトを示す。最後に，それを実現するための実装方法の検討を行った。

キーワード：PBNM，ネットワーク管理，クラウド，アクセス制御，Destination NAT

1. はじめに

現在のインターネットは，自律分散型ネットワークである。その為，統一的にインターネット全体を安全・効率的に管理するための仕組みが存在していない。それ故，インターネットの仕組みをあまり理解していない利用者がインターネットに接続する場合には，「個人情報の漏洩」，や「ネットワーク攻撃の踏み台利用」が発生する危険性が高くなる。その一方で，インターネット全体をある一定の管理状態に置くための研究は，著者の知る範囲では，現在行われていない。そこで，PBNMの考え方をインターネット全体に適用して管理する「インターネットPBNM（図1の右側）の研究」を長期的視野に立ち推進し，安全・効率的に管理されるインターネットの実現を目指している。これまでの所，図1の4ステップで研究を進めており，本研究は（Step3）に相当する研究である。

図1の（Step1）に該当する既存PBNM（図2）の研究では，自組織のネットワーク・セキュリティポリシーに基づくネットワーク管理を実現する方法を確立されている。具体的には，サーバとクライアントの間の経路上に配置される通信制御機構（PEP）による通信制御（アクセス制御，通信の暗号化，QOS制御など）を通して自組織ネットワーク全体を管理す

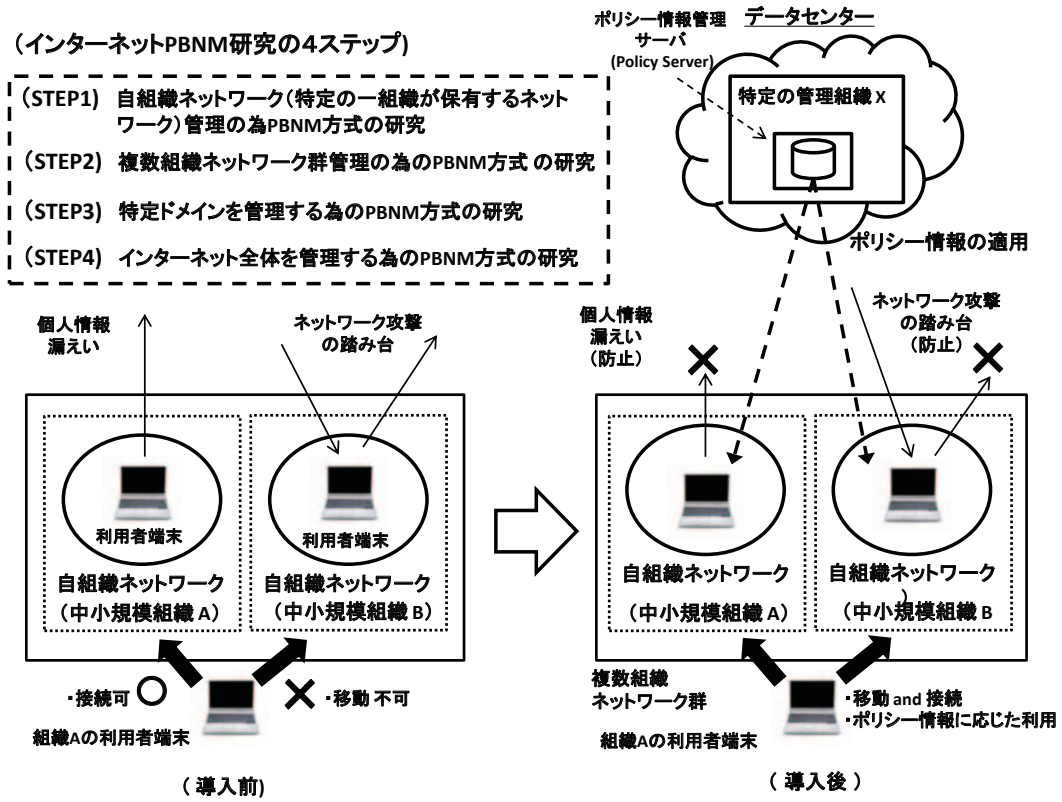

図1　インターネットPBNM

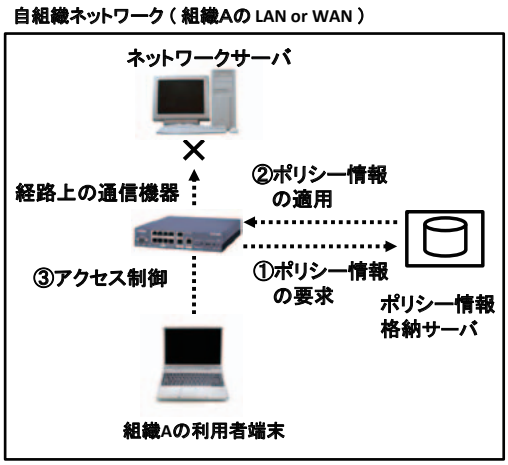

図2　既存PBNM

る。この方法は，IETF（R. Yavatkar at el. IETF RFC 2753, 2000）やDMTF（DMTF, DSP0123,2002）など複数の組織で標準化されている。この既存PBNMは，元々，自組織ネットワークを管理する為のものであるが，理論的・技術的には，（Step2）に該当する「複数組織ネットワーク群」の管理にも応用することは可能である。しかしながら，研究論文として報告されておらず，PBNMの技術的構成要素であるアクセス制御[1]やQOS

制御 [2] を個別に研究対象として取りあげて，複数組織で利用する為の研究が若干報告されているのにとどまっている。

そこで，著者は，(Step2) の研究を推進し，PBNM方式の適用領域を，個別組織から複数組織に拡大し，複数組織ネットワーク群管理の為の方式を確立した。そこで，本論分では，更に適用領域を拡大する（Step3）の研究に相当する「特定のドメインを管理する方式」を提案する。

既存PBNMは，PEPをネットワーク経路上に配置する為，ある管理組織が他組織ネットワークを管理しようとする場合，他組織が保有するネットワーク機器を変更する必要があり，(a) 機器変更によるコストの発生，(b) 既存PBNMの適用時に発生する可能性があるネットワークトポロジ変更，(c) 他組織による自組織ネットワーク機器の変更時に問題となるセキュリティポリシーやネットワークポリシー上の制限，という問題点により，機器変更が不可能な場合がある。インターネット全体の管理を前提とする場合は適用対象のネットワーク数が不特定の膨大な数となる為，　これらの問題点，特に，(c) の問題点が致命的となり，全ての組織へ導入するのは困難となる。

そこで，図1の（Step1）として，サーバとクライアント上に配置するソフトウェアのみで実現可能（＝ネットワーク上の物理的機器に対する変更が不要）となる「ネットワーク機器の変更が不要な自組織ネットワーク管理のPBNM方式」を実現する為，ソフトウェア形態のPEP（DACS Client）を物理クライアント・仮想化クライアントに配置する「DACS（Destination Addressing Control System）方式」を確立し，更に，(Step2) の「複数組織ネットワーク群のPBNM管理」を実現する「クラウド型PBNM方式」を確立する研究を進めている。(Step1)では，①方式の原理提案，②Virtual Private Network（VPN）を用いたPEP非配置の物理クライアントからの通信に対するアクセス制御機能，③物理クライアントの台数増加による処理負荷シミュレーション，④DACS方式実現の為のソフトウェア開発などの研究を行った。(Step2) では，①複数組織管理の為の方式の確立，具体的には，原理提案，実装，評価 を実施した。

2. 研究の動機と関連研究

既存のネットワーク管理に関する研究・技術としては，例えば，ユーザ認証に関する研究 [1] やサーバ負荷分散などの負荷分散に関する研究 [2]，VPN (Virtual Private Network) [3] のようなネットワーク仮想化に関する研究，あるいは，ネットワーク接続時のセキュリティ保証のための検疫ネットワーク [4] に関する研究など様々な研究が為されている。これらの研究は，それぞれある特

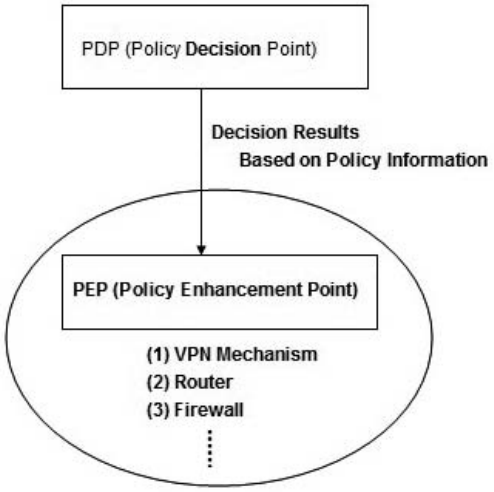

図3　IETFにおけるPBNM

定の個別の目的について研究が行われており，あるネットワーク全体を安全かつ効率的に管理することを目的としている訳ではない。あるネットワーク全体を安全かつ効率的に管理する為の研究の一つとして，IETF（Internet Engineering Task Force）で示されているポリシーに基づくネットワーク管理（PBNM）の研究［6］［7］［8］［9］が存在する。このPBNMの原理は，図3に示された内容のものである。

具体的には，PDP（Policy Decision Point）と呼ばれる判断機能の作用として，ポリシー情報に基づいて通信の許可や遮断などの判断が行われる。その後，その判断の結果が，サーバやクライアントなどのホスト間のネットワーク系路上に配置された通信制御の為の仕組み（制御点），例えば，VPN装置，Router，Firewall などの上に配置されるPEP（Policy Enforcement Point）と呼ばれる場所に通知・伝達され，その判断に基づいて通過しようとする通信に対して制御が加えられる仕組みである。また，このPBNMと同様に，ネットワーク経路上にアクセス制御の為にゲートウェアシステムを用いて利用者単位でアクセス制御するOpengate［5］に関する研究も行われている。（Opengateは，ある国立大学において，学内ネットワークを管理する目的で研究・開発が為されたものである。）

これら方式の問題点として，次の（1）～（2）の2点をあげることが出来る。

（1）多数のクライアントから発信される通信をネットワーク経路上に配置した装置・仕組みでまとめて制御する方式である為，非常に処理負荷が高くなる点。

（2）各ホスト間に通信制御の為の装置・仕組みが必要である為，ネットワークシステムの構成によっては，その装置・仕組みを追加する為の構成変更が必要になる点。

そこで，これらの問題点を克服する新しいネットワーク管理の方式を提案し，DACS方式[11][12]と呼んでいる。詳細は後述するが，このDACS方式の基本原理は，PBNMにおけるPEPに相当するソフトウェアをクライアントに配置する

方式である。ソフトウェアの通信制御の為の機能であるパケットフィルタリングとDestination NATの仕組みを用いてクライアントから発信される通信を制御する。その通信制御を通してネットワーク全体を管理する方式である。クライアントにPEPに相当するソフトウェアを配置するという観点で考えると，PBNMの研究の中には，クライアントにソフトウェアを配置してQOS制御する方式の研究［10］もある。しかしながら，これまでの研究で，クライアントにPEPに相当するソフトウェアを配置してネットワーク全体を効率的に管理する目的の研究は，DACS方式以外に見当らない。

3. 既存DACS方式の概要説明

本章では，既存のDACS方式の要約を記述する。具体的には，過去に発表した論文［11］［12］の要約である。

3.1. 基本機能の説明

DACS 方式の原理は，ネットワークに接続したクライアントの通信をユーザ，またはクライアント単位で制御することによって，ネットワークシステム全体を管理することである。具体的な制御内容は，通信先サーバを変更する，あるいは，通信を遮断することである。これらは，ネットワーク管理者により通信制御情報を管理するサーバ（以下，通信制御情報管理サーバ）に設定された通信制御の為のルール（以下，通信制御ルール）に基づいて制御される。通信先サーバを変更する為には，クライアント上にDestination NATを配備し，通信制御情報管理サーバに定められたルールに従って宛先を変更する。通信を遮断する為には，クライアント上にパケットフィルタリングの仕組みを設けて，同様に通信制御情報管理サーバに定められたルールに従って通信を遮断する。DACS 方式では，これらの原理に基づき，以下の基本機能をユーザ，又は，クライアント単位で実現する。

（a）同一ホスト名に対する通信先サーバ切換
（b）利用サービス制限
（c）アクセスポート許可

ユーザ単位で通信制御する為には，ユーザ認証サーバと組み合わせることにより，あらかじめ通信制御情報管理サーバに設定されたユーザ単位の通信制御ルールに従ってクライアント上でDestination NAT による宛先変更を行うか，パケットフィルタリングの仕組みにより通信を遮断する。同様に，クライアント単位で通信制御する為には，通信制御情報管理サーバに設定されたIP アドレス単位の通信制御ルールに従い通信制御を行う。それにより，ある特定の場所に設置したクライアントに対する通信制御が可能になる。但し，その通信制御の前提条件として，原則的にはクライア

ントに固定IP アドレスを設定する必要がある。DHCP 環境下においては，ネットワーク単位，あるいは，サブネットワーク単位で接続されたクライアントに同一の制御をすることは可能である。又，通信制御情報管理サーバには，ユーザ，及び，クライアント単位の通信制御ルールが両方設定されている為，そのユーザでログインしたクライアントを制御する為のルールが重複してしまう場合は，ある一定の処理法則に従い優先するルールを決めて通信制御を行う。その処理法則は，各組織毎に定められるネットワークポリシーにより決定される。

3.2. 基本システム構成

図4に，DACS方式における基本的なシステム構成の全体像を示す。同図のDACS SV（DACS Server） はDACS方式によるサービスを提供する為に必要なサーバ機能であり，通信制御情報管理サーバの役割も果たす。DACS CL（DACS Client）は，サービスの提供を受ける為に必要なクライアント機能である。又，DACS CTL（DACS Control）は，DACS CLの一部であり，実際に通信を制御する通信制御サービスの役割を果たす。更に，DACS rulesは，前節で説明した（a）～（c）の3つの基本機能による通信制御の為に必要なルールであり，次の（A）（B）で構成される。（以下の宛先情報X,Y,Zは，IPアドレスとポート番号である。）

（A）（a）の機能を制御する為に，Destination NATに必要となる通信先変更前の宛先情報X と通信先変更後の宛先情報Y。

（B）（b）（c）の機能を制御する為，パ

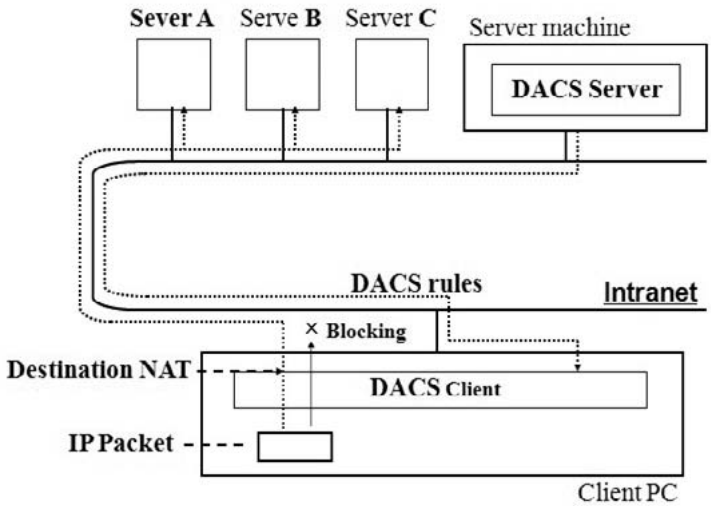

図4　DACS方式の基本システム構成

ケットフィルタリングで通信の遮断や許可をする為に必要となる通信の宛先情報Z。

そのDACS rules は，DACS SV からDACS CLへ送信された後，DACS CLの一部であるDACS CTLに適用される。そして，DACS CTLでは適用直後から通信制御が行われる。ここでは，DACS SVは常時定常状態（運用状態）であり，ネットワークの通信が問題なく行える状態であるとの前提のもと，DACS CLの基本的な処理の流れと内容を説明する。また，DACS CLは，クライアントOS の起動・終了処理の一部として起動・終了させる。

また，DACS SV･CL･CTLのレイヤー設定を図5に示す。サーバ，及び，クライアントのアプリケーション層に配置されたDACS SV とDACS CL間でDACS rulesを送受信する（a)。DACS rulesを受信したDACS CLは，DACS CTLに対してDACS rulesを適用する（b)。DACS rulesが適用されたDACS CTLは，ネットワーク層に配置されている。クライアント上で,Webブラウザやメーラーなどのネットワークアプリケーションが起動され，それらのアプリケーションの通信が，クライアント外部に流れる前に，Destination NATによる通信先サーバ変更やパケットフィルタリングにより通信遮断の処理が行われる（c)。

3.3. VPN機能

DACS方式は，クライアントに配置したDACS CLで通信を制御する方式である。その為，DACS CLを配置していないクライアントをネットワークに接続する場合，ネットワークサービスを自由に

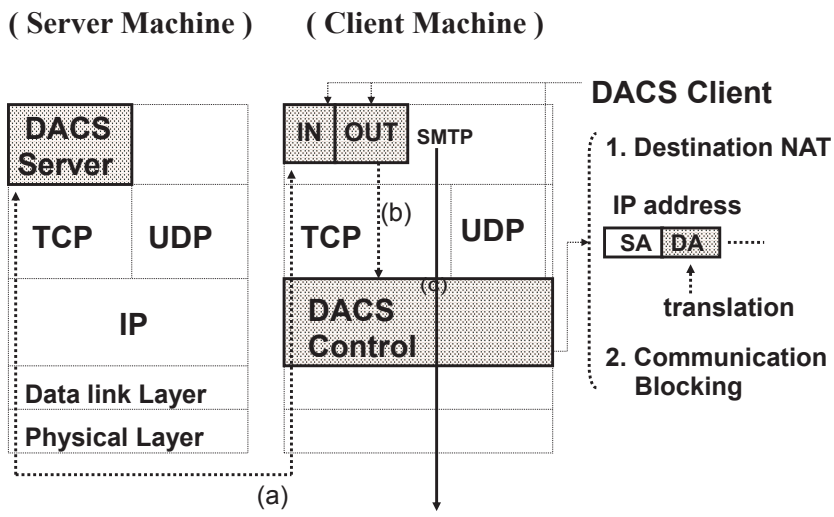

図5　レイヤー設定

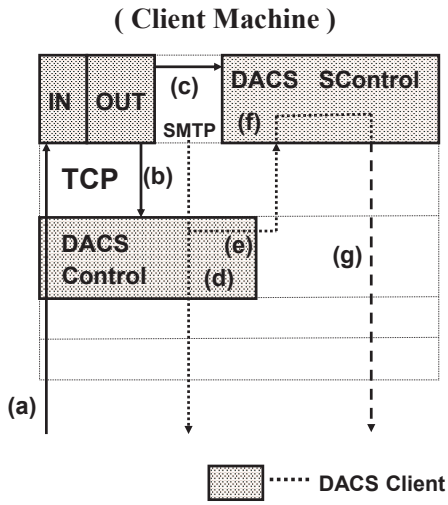

図6　VPN機能

利用出来てしまうという問題点がある。セキュリティポリシーやネットワークポリシーによっては，そのようなクライアントが接続するのを許可する場合もあり得るが，不許可の場合に備えて対処する必要がある。図6に示したように，クライアントから発信される通信をVPN（Virtual Private Network）化出来るように機能拡張し，VPN化されないクライアント，つまり，DACS CLを配置しないクライアントからの通信を遮断出来るようにして対処する。具体的な仕組みを図6に従って説明する。まず，通信制御開始前に必要な初期化処理を説明すると，(a)のように，DACS SVからDACS rulesがDACS CLに対して送信された後，（b）のようにDACS CTLにDACS rulesが適用されると同時に，（c）のようにVPN化する機能であるDACS SCTL（DACS SControl）にDACS rulesが適用されて，初期化処理が完了する。そして，（d）のようにクライアントアプリケーションから通信が発信されると，DACS CTLの制御によって，(e)のようにlocalhostへ宛先が変更される。その通信を受け取ったDACS SCTLの制御によって，(f) の部分で通信がVPN化されて，（g）のように，その通信がクライアント外部へ発信される。

4. DACSシステムの実装方法

4.1. 実装上のポイント

（1）開発システムの環境

a. DACS SV

動作OS: Fedora Core 2

開発言語: Visual C++ 7.1

b. DACS CL

動作OS: Windows XP Professional Edition

開発言語: Visual C++ 7.1,

Winsock2 LSP（DACS Control）

その他: Putty（DACS SControl）

（2）DACS SVとDACS CL間の通信

DACS rulesの送受信などのDACS SVとDACS CL間は，TCP/IPのソケット通信を用いて実現している。

（3）クライアント上での通信制御部

今回は，Windowsクライアント上で動作するDACS CL を実装した。DACS Controlの機能として必要な宛

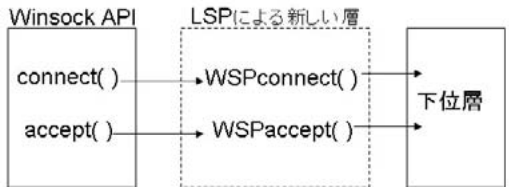

図7　Winsock2 LSP

先NATとパケットフィルタリング機能は，Microsoft社のWinsock2 LSP（Layered Service Provider）を用いて実装した。Winsock2 LSPとは，図7に示したように，もともと存在しているWinsock APIとその下位層の間に設けられる新しい層である。具体的は，クライアントソフトウェアがサーバ接続時に実行されるconnect（）の中で呼び出されるWSPconnect（）の内部に宛先NATの処理とクライアントから発信される通信に対するパケットフィルタリング処理を組み込んでいる。また，クライアントへの通信を受信する際にクライアント側で実行されるaccept（）の中で呼び出されるWSPaccept（）の内部に，クライアント外部から着信する通信に対するパケットフィルタリングの処理を組み込んでいる。

（4）VPN通信

通信をVPN化する為のVPNクライアント，つまり，DACS SControlは，フリーソフトウェアのPuttyの機能を流用して実現した。クライアントから発信される通信のうちでVPN化する必要がある場合は，上記の宛先NATで通信の宛先をLocalhostへ変更する処理を施し，それ以降は，Puttyがその通信を受信してポートフォワーディング機能によりVPN通信を発信する。

5. 提案方式の実装方法の検討

第3章で説明した既存のDACS方式のDACS SVをクラウド上に配置して，複数の組織が各々保有するネットワークの集まり（ネットワークグループ）を管理する方式［13］に関する研究を過去に行っている。

本提案方式は，その方式で管理されるネットワークグループがインターネット上に複数存在した状態で，お互いに自律的にポリシー情報のやり取りなどを行うことで，管理範囲を一定の範囲（ドメイン）に拡大するものである。図8において，その概念が説明される。組織A（Org.A）と組織B（Org.B）を管理する為の論理的範囲として，ネットワークグループ1が存在する。同様に，組織C（Org.C）と組織D（Org.D）を管理する為の論理的範囲として，ネットワークグループ2が存在する。本提案方式では，それらのような複数のネットワークグループ全てを管理対象とする。前述の既存の方式では，1つのネットワークグループには，1つの管理組織が存在する。その為，複数のネットワークグルー

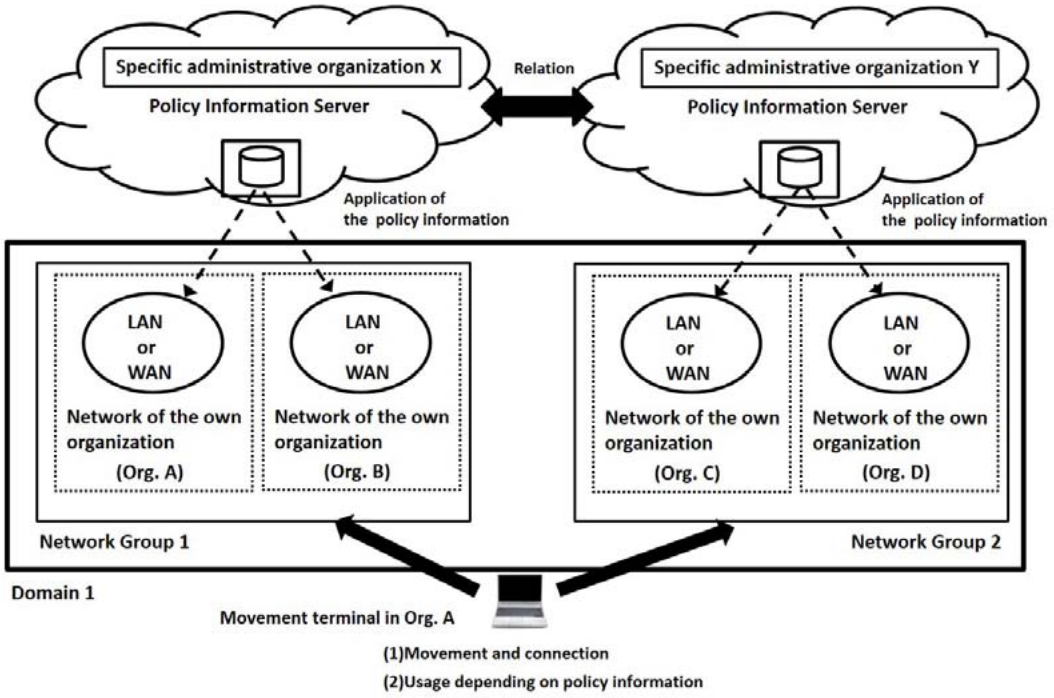

図8　提案方式の概念

プが存在する場合，管理組織も同じ数だけ存在することになる。それらの管理組織を統括管理する1つの組織を設けることも，論理的には可能であるが，インターネットが1つの管理組織で管理される形にはなっていない為，インターネットとの親和性を確保する為に，1つの管理組織を設けることはしない。複数の管理組織が，自律的に分散配置され，お互いに協調関係を結ぶことにより，管理する方式として研究を進める。具体的には，個々のネットワークグループ内に，1つのポリシーサーバーを設けて，個々の管理組織が，自分のネットワークグループの中の組織のユーザ情報とポリシー情報を管理する。例えば，Network Group1の中のOrg.Aに所属するユーザAが，別のネットワークグループであるNetwork Group2に所属するOrg.Cが保有するネットワークを利用する場合には，Network Group2の管理組織Yから，Network Group1の管理組織Xに対して，ユーザAのポリシー情報を問い合わせて取得する。その上で，Network Group2に予め登録されたポリシー情報と照合させる形で，最終的なポリシー情報を決定し，ユーザAがNetwork Group2内で使用するクライアントに，

ポリシー情報を適用し，通信制御が行われる。このような方式とすることで，特定のネットワークグループ内だけではなく，複数のネットワークグループをユーザが移動する場合でも，ある一定の管理状態を保つPBNM方式が実現されると考えている。

このような方式を実現する為に，既存方式を実現する為のソフトウェア（DACS SV・DACS CL）に以下のような機能を加える形での実装を行う必要があると現時点では考えている。

(1) Public Key Infrastructure（PKI）による通信の暗号化機能
(2) ある組織のユーザが，別組織のネットワークへアクセスする場合の認証機能（そのユーザが所属する組織が保有する認証サーバを用いて，認証を行う機能）
(3) 各ネットワークグループの管理組織が保有するDACS SVの間でポリシー情報をお互いに交換する機能
(4) 複数種類のポリシー情報（ユーザ別のポリシー情報，各組織のネットワーク内で共通のポリシー情報，各ネットワークグループ内で共通のポリシー情報など）が重複する場合に，優先順位の判定を行う為のルール設定を行う機能，その設定ルールに基づき適用するポリシー情報を決定・生成する機能

既存方式に対して，最低限，これらの機能を付加する形で実装を行う必要があると考えている。

6. まとめ

本研究ノートでは，既存のDACS方式を応用する形で，管理対象のネットワーク領域を拡張する為に必要となる実装方法について検討した。既存のDACS方式を実現する為に開発したソフトウェア（DACS SV･DACS CL）に，最低限4つの機能（PKIによる通信の暗号化機能・ユーザが所属する組織側で行うユーザ認証機能・ネットワークグループ間でのポリシー情報交換機能・ポリシーの優先順位設定機能に基づく最終的なポリシー情報の生成機能）を付加する形で実装を行う必要がある旨を示した。今後は，提案方式実現に向けたソフトウェア実装を進め，機能実験に基づく評価・処理負荷実験に基づく評価を実施する予定である。

参考文献

[1] 若山公威，出路裕介，冷基立，岩田彰，“指紋照合によるリモートユーザ認証方式，”情報処理学会論文誌，Vol.44, No.2, pp.401–404, 2003.

[2] 下川俊彦，木場雄一，中川郁夫，山本文治，吉田紀彦，“広域分散環境におけるDNSと経路情報を利用したサーバ選択機構，”電子情報通信学会論文誌B, Vol.J86-B, No.8, pp.14541462, 2003.

[3] C.Metz, “The latest in virtual private

networks: part I," IEEE Internet Computing, Vol.7, No.1, pp.87–91, 2003.

[4] http://www.nec.co.jp/univerge/solution/pack/quarantine/

[5] 只木進一，江藤博文，渡辺健次，渡辺義明，“利用者移動端末に対応した大規模ネットワークのOpengateによる構築と運用，”情報処理学会論文誌，Vol.46, No.4 pp.922–929, 2005.

[6] S.Jha, M.Hassan, “Java implementation of policy-based bandwidth management,” Int. J. Network management, John Wiley&Sons, Vol.13, isuue.4, pp.249–258, July, 2003.

[7] G.M.Prerez, F.G.Skarmeta, S.Zeber, T.Symchych, “Dynamic Policy-Based Network Management for a Secure Coalition Environment,” IEEE Communications Magazine, Vol.44, issue.11, pp.58–64, November, 2006.

[8] D.C.Verma, “Simplifying Network Administration Using Policy-Based Management,” IEEE Network, Vol.16, issue.2, pp.20–26, March-April, 2002.

[9] 菅野政孝，田中俊介，坂田祐司，小熊慶一郎，白鳥則郎，“情報ネットワークシステムのポリシー制御”PolicyComputing”の適用と実装，”情報処理学会論文誌，Vol.42, No.2, 2001.

[10] H.Chaouchi, P.M.Antunes, “Pre-handover signaling for QOS aware mobility management,” Int. J. of Network management, John Wiley&Sons, Vol.14, isuue.6, pp.367–374, November, 2004.

[11] K.Odagiri, R.Yaegashi, M.Tadauchi, N.Ishii, “Efficient Network Management System with DACS Scheme: Management with communication control,” Int. J. of Computer Science and Network Security, Vol.6, No.1, pp.30–36, January, 2006.

[12] K.Odagiri, R.Yaegashi, M.Tadauchi, N.Ishii, “Secure DACS Scheme,” Journal of Network and Computer Applications,” Elsevier, Vol.31, No.4, pp.851–861, November, 2008.

[13] K. Odagiri, S. Shimizu, N. Ishii, “Functional Evaluation of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations,” International Journal of Networked and Distributed Computing (IJNDC), Volume 5, Issue 2, pp.62–70. April, 2017.